TP Auth

Manipuler les JWT et mettre en place un contrôle d'accès

Objectif

L'objectif de ce TP est de créer un service d'accès à des posts (contenu textuel) avec contrôle d'accès.

Utilisateurs

Ci-dessous l'ensemble des utilisateurs pouvant s'authentifier.

ID	Pseudo	Admin
777	admin	true
123	bob	false
321	alice	false

Vous avez le choix du mot de passe à utiliser pour chaque utilisateur.

Spécifications fonctionnelles

Cette section décrit l'ensemble des spécifications fonctionnelles liées au service.

Génération de JWT

Le service doit exposer un moyen de générer et d'obtenir un JWT valable pour un utilisateur. Le JWT doit avoir une durée de **validité de 1 jour**.

*Bien sûr, seul un utilisateur **authentifié** peut demander la génération et l'obtention de son token...*

Accès aux ressources

Le service doit exposer un moyen de **consulter** des posts (ressources). Ci-dessous l'ensemble des posts accessibles.

ID	Auteur	Contenu
456	123 (bob)	*ce que vous voulez*
654	321 (alice)	*ce que vous voulez*
555	777 (admin)	*ce que vous voulez*

Les utilisateurs **non-admin** n'ont accès qu'aux posts dont ils sont l'auteur. Par exemple, bob n'a accès qu'au post 456 et alice qu'au post 654.

Les utilisateurs **admin** ont accès à tous les posts.

Contraintes techniques

Aucune contrainte technique n'est imposée. C'est à vous de faire les choix techniques qui vous semblent les plus judicieux tout en respectant au maximum les bonnes pratiques liées à REST.

Aucun langage, framework ou bibliothèque n'est imposé.

Toutes les réponses doivent être en `application/json`.

Par soucis de simplicité, le service d'authentification (génération de token) et le service d'accès aux posts sont exposés sur un seul et même serveur via une API REST. La création d'un seul projet est donc suffisante.

Également par soucis de simplicité, les informations liées aux utilisateurs et aux posts peuvent directement être stockées dans des fichiers sur le serveur. Les mots de passe des utilisateurs peuvent être stockés en clair **MÊME S'IL NE FAUT JAMAIS LE FAIRE EN PRATIQUE**.

Modalités d'évaluation

Vous êtes notés sur le respect des spécifications (ci-dessus) et des bonnes pratiques liées à REST (quelques détails ci-dessous).

- **Fonctionnel**
  - La génération du JWT
  - L'accès aux posts
    - **Contrôle d'accès !**
- **Technique**
  - Choix des méthodes HTTP à utiliser
  - Choix des vecteurs d'informations

Pour la technique, vous êtes notés seulement sur la partie "Controller". Vous **n'êtes pas** notés sur la partie "Service" (logique, implémentation).